the transmission apparatus of the cryptocommunication system of claim 1 are defined to perform, and the transmission apparatus recited in claim 18 performs the same operations of the elements of the transmission apparatus of the cryptocommunication system of claim 1.

Outline of Response

The transmission apparatus of the cryptocommunication system of claim 1 includes constituent elements X and Y.

1. A first assumption is made that Dai discloses a technology corresponding to element X. Under this first assumption, the Applicants will demonstrate that Dai does not disclose or suggest a technology corresponding to element Y.

2. A second assumption is made that Dai discloses a technology corresponding to element Y. Under this second assumption, the Applicants will demonstrate that Dai does not disclose or suggest a technology corresponding to element X.

According to this method of demonstrating that Dai fails to disclose or suggest each and every limitation of the transmission apparatus of claim 1, the Applicants will establish that Dai can only reasonably be interpreted as disclosing either element X or Y, and that the transmission apparatus of claim 1 is clearly distinguishable and novel over the technology disclosed in Dai.

The Invention of Claim 1

The transmission apparatus of the cryptocommunication system of claim 1 includes first operation means for performing an invertible operation on the plaintext and the first additional information to generated connected information. The transmission apparatus of claim 1 also includes encrypting means for encrypting the connected information according to an encryption algorithm so as to generate the ciphertext.

The reception apparatus of the cryptocommunication system of claim 1 includes decrypting means for decrypting the ciphertext according to a decryption algorithm, which is an inverse-conversion of the encryption algorithm, so as to generate decrypted connected information. The reception apparatus of claim 1 also includes second operation means for performing an inverse operation of the invertible operation on the decrypted connected information and the second additional information so as to generate the decrypted text.

Dai discloses a cryptographic system which includes an encoder 22 (transmission apparatus) and a decoder 24 (reception apparatus). The encoder transforms a message M into ciphertext C and transmits the ciphertext C over a communications channel 26 to the decoder 24 (see Figure 1 and Column 2, lines 31-55).

Comparison and Analysis of Claim 1 and Dai Under First and Second Assumptions

(1) Comparison and Analysis Under First Assumption

Dai discloses that the message M is encrypted by using a value W, where "[t]he value W is encoded as a function of a value $h_1(x)$ and the message M (e.g. $h_1(x)$ xor M) (see Column 2, lines 48-50, where "xor" is an exclusive OR function; and see Column 3, lines 58-67).

"xor" is considered to correspond to an encryption algorithm. In view of this, under the first assumption, the value W = $h_1(x)$ xor M corresponds to the encrypting means of claim 1.

Under this first assumption, the encoder 22 disclosed in Dai transmits the ciphertext C that includes the value W. Therefore, under this first assumption, Dai does not disclose or suggest a technology of generating the connected information from the message M because Dai does not perform any other operations on the message M. That is, under the first assumption, Dai cannot be reasonably interpreted as disclosing "first operation means for performing an invertible operation on the plaintext and the first additional information to generate connected information," as recited in claim 1.

The cryptocommunication system of claim 1 produces a novel and advantageous effect of generating ciphertext whose security level is high, by providing the first operation means for performing an invertible operation on the plaintext and the first additional information to generate connected information, and the encrypting means for encrypting the connecting information to generate encrypted connected information.

Under this first assumption, it is assumed that the value W = $h_1(x)$ xor M corresponds to the encrypting means of claim 1. Under this first assumption, Dai cannot reasonably be interpreted as disclosing the first operation means of claim 1 for the following reasons.

Using this first assumption, suppose that a third party intercepts the ciphertext C that is generated according to the system of Dai. Under this first assumption, Dai does not disclose or suggest a technology of generating the connected information from the message M because Dai does not perform any other operations on the message M. As a result, Dai cannot prevent the third party from obtaining the message by decrypting the ciphertext C, since Dai does not disclose or suggest a technology of the connected information from the message M because Dai does not perform any other operations on the message M. Accordingly, Dai cannot reasonably be interpreted as disclosing or suggesting "first operation means for performing an invertible operation on the plaintext and the first additional information to generate connected information," as recited in claim 1.

(2) Comparison and Analysis Under Second Assumption

In line 6 on page 5 of the Office Action, the Examiner alleged that "x" corresponds to the first additional information of claim 1. If this is assumed to be the case, the value $W = h_1(x)$ xor M corresponds to the invertible operation of the first operation means of claim 1, and the value W corresponds to the connected information.

However, under this second assumption, the encoder 22 of Dai does not perform any operation whatsoever with respect to the value W, and therefore, the value W is transmitted without being encrypted. Therefore, if $W = h_1(x)$ xor M is considered to correspond to the invertible operation of claim 1 and the value W is considered to correspond to the connected information of claim 1, Dai cannot be reasonably interpreted as disclosing an "encrypting means for encrypting the connected information according to an encryption algorithm so as to generate the ciphertext," as recited in claim 1, since Dai performs no operation whatsoever with respect to the connected information W.

Accordingly, under this second assumption, the value W will be transmitted without being encrypted, and as a result, the system of Dai cannot maintain the secrecy of the transmitted information.

In contrast to Dai, the transmission apparatus of claim 1 includes <u>both</u> the first operation means <u>and</u> the encrypting means. As a result, information that is to be transmitted is made secret because of being encrypted by the encrypting means before the information is transmitted. In addition, the encrypting means of claim 1 encrypts connected information, and therefore is able to prevent the third party that has intercepted the ciphertext from obtaining the corresponding message, even if the intercepted ciphertext has been successfully decrypted.

Thus, the invention of claim 1 has an effect of generating ciphertext whose security level is high, and therefore, the invention of claim 1 has marked technological advantages over the system disclosed in Dai.

(3) Summary of the Comparison and Analysis Under the First and Second Assumptions

As described above, if "the value $W = h_1(x)$ xor M" is assumed to correspond to the encrypting means of claim 1, Dai clearly fails to disclose or suggest the first operation means of claim 1 since Dai does not disclose or suggest generating the connected information from the message M, as Dai does not perform any other operations on the message M. Therefore, under the first assumption, Dai cannot be reasonably interpreted as disclosing first operation means for performing an invertible operation on the plaintext and the first additional information to generate connected information, as recited in claim 1.

On the other hand, if, under the second assumption, "the value $W = h_1(x)$ xor M" is assumed to correspond to the first operation means of claim 1, Dai fails to disclose or suggest the encrypting means of claim 1, since Dai performs no operation whatsoever with respect to the connected information W. Accordingly, if "the value $W = h_1(x)$ xor M" is assumed to correspond to the first operation means of claim 1, Dai cannot be reasonably interpreted as disclosing encrypting means for encrypting the connected information according to an encryption algorithm so as to generate the ciphertext, as recited in claim 1.

In view of the above, Dai clearly does not disclose or suggest a combination of the first operation means and the encrypting means of claim 1. Similarly, Dai does not disclose or suggest a combination of the first operation means and the encrypting means of the transmission apparatus of claim 18.

Furthermore, for the foregoing reasons, Dai clearly does not disclose or suggest a combination of operations of performing an invertible operation on the plaintext and the first additional information to generate connected information, and encrypting the connected information according to an encryption algorithm so as to generate the ciphertext, as recited in the method and programs of claims 15-17.

Accordingly, the inventions of claims 1 and 15-18 are clearly not anticipated by Dai since Dai does not disclose each and every limitation of claims 1 and 15-18.

Furthermore, one skilled in the art would not have been motivated to modify the system of Dai to provide for either the first operation means or method and program element of claims 1 and 15-18 or the encrypting means or method and program element of claims 1 and 15-18 to arrive at the inventions of claims 1 and 15-18.

Accordingly, claims 1 and 15-18 are clearly not anticipated or rendered obvious by Dai since Dai fails to disclose or suggest each and every limitation of claims 1 and 15-18.

Therefore, claims 1 and 15-18 are clearly allowable over Dai.

In item 8 on page 6 of the Office Action, claim 2 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Wel Dai in view of Jones (5,412,730). As demonstrated above, Dai clearly fails to disclose or suggest the first operation means <u>and</u> the encrypting means of claims 1 and 18, as well as the corresponding operations of the program and method of claims 15-17.

Jones also fails to disclose or suggest the first operation means and encrypting means of claims 1 and 18 as well as the corresponding operations of the program and method of claims 15-17.

Therefore, Jones fails to cure the deficiencies of Dai for failing to disclose or suggest each and every limitation of claims 1 and 15-18.

Accordingly, no obvious combination of Dai and Jones would result in the inventions of claims 1 and 15-18 since Dai and Jones, either individually or in combination, clearly fail to disclose or suggest each and every limitation of claims 1 and 15-18.

Furthermore, it is submitted that the clear distinctions discussed above are such that a person having ordinary skill in the art at the time the invention was made would not have been motivated to modify Dai and Jones in such as manner as to result in, or otherwise render obvious, the present invention as recited in claims 1 and 15-18. Therefore, it is submitted that the claims 1 and 15-18, as well as claims 2-14 and 19 which depend therefrom, are clearly allowable over the prior art as applied by the Examiner.

In view of the foregoing remarks, it is respectfully submitted that the present application is clearly in condition for allowance. An early notice thereof is respectfully solicited.

If, after reviewing this Request, the Examiner feels there are any issues remaining which must be resolved before the application can be passed to issue, the Examiner is respectfully requested to contact the undersigned by telephone in order to resolve such issues.

Respectfully submitted,

Masato YAMAMICHI et al.

By: Jonathan R. Bowser
Jonathan R. Bowser
Registration No. 54,574
Attorney for Applicants

JRB/nrj
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
February 10, 2006